MODEL STRATEGIJE GRADNJE VARNIH SISTEMOV POSLOVNE INTELIGENCE

Stanka Šalamun
Direktorica operacij, ACROS d.o.o.
security@acrossecurity.com

Povzetek

Številni odkriti vdori v nekatere tudi najbolj varnostno kritične inteligentne poslovne sisteme v zadnjih letih so znamenje, da aplikacije, ki jih sestavljajo, niso načrtovane, grajene, preizkušene in vzdrževane na način, da bi vzdržale tudi najbolj osnovne napade. Organizacije se v ključnem obdobju - pri gradnji programske opreme - srečujejo s kompleksnostjo svojega informacijskega sveta ter z nepoznavanjem in pomanjkljivim izvajanjem dobrih praks varnostnega procesnega inženiringa. Trenutni varnostno-informacijski standardi za boj proti vedno bolj motiviranim in naprednim napadalcem na programsko opremo so vse premalo konkretni ali vse preveč zapleteni za preprosto vsakdanjo rabo, prav tako ni široko uporabnih formalnih modelov, ki bi glede na varnostne zahteve omogočili njihovo sistematično in enovito varnostno obdelavo, zato smo izdelali predlog formalnega modela za opis aktivnosti sistematične gradnje varne programske opreme, ki je predvsem preprost, konkreten, uporaben za obdelavo velikega števila aplikacij in ki omogoča primerjavo. Pomembna pridobitev modela je seznam zahtevanih varnostnih aktivnosti po prioritetah na ciljnem varnostnem nivoju. S tem smo definirali preprosto strategijo, ki vodi k željenemu varnostnemu nivoju vsake posamezne aplikacije in celotnega sistema poslovne inteligence.

Model smo v praksi preizkusili na enem največjih bodočih sistemov poslovne inteligence v Sloveniji – informacijskih sistemih v javni upravi. Na enoten način smo klasificirali varnostne zahteve v javnih naročilih za sisteme poslovne inteligence v javni upravi, določili ciljne varnostne nivoje ter ugotovili obstoječe ter pomanjkljive varnostne prakse pri naročanju. Ocenjujemo, da gre za prvo tovrstno analizo na področju Slovenije, ki bi jo napredna slovenska informacijska družba zagotovo morala spoznati.

Abstract

THE MODEL FOR APPLICATION SECURITY STRATEGY IN BUSINESS INTELLIGENCE SYSTEMS

In the last few years majority of intrusions into business intelligence systems have been caused by application flaws, which indicates a concerning fact that building secure business intelligence systems is still a hard-to-achieve goal The article gives an introdution of an evaluation model for defining an application security target level as well as methodology for evaluating the actual level of implemented application security in complex and data-rich business intelligence systems.

Ključne besede

Aplikacijska varnost, aplikacijska varnostna strategija, poslovna inteligenca, aplikacijski varnostni življenjski cikel, aplikacijske varnostne metrike

Key words

Application secucrity, application security strategy, business intelligence, application security lifecycle, application security metrics

1. UVOD

Če so prej neslavno prvo mesto zasedali vdori zaradi slabo vzdrževanih računalniških omrežij, uporabe koncepta »varnosti s skrivanjem« in neusposobljeni uporabniki računalniških sistemov, je programska oprema, ki ne vzdrži napadov, danes najpogostejša vstopna vrata v sisteme poslovne inteligence tudi nekaterih varnostno najzahtevnejših organizacij.

Razlogov za to je več. Kompleksnost računalniškega sveta je izrazito narasla, saj so operacijski sistemi, podatkovne baze in drugi aplikacijski svet sestavljeni iz vedno več vrstic kode, ki jih je nemogoče nadzorovati - od tod vedno več varnostnih napak. Prav tako je meja med zunanjim (Internetom) in notranjim (Intranetom) računalniškim svetom skoraj izginila in tako izbrisala močno linijo obrambe, ki so jo morale na svoja pleča prevzeti vmesniki programske opreme - vstop od zunaj v notranje omrežje organizacij in do src najbolj kritičnih podatkovnih strežnikov še nikoli ni bil tako preprost. Tudi podatki so vedno bolj mobilni, saj je postala poslovna potreba, da jih na prenosnih računalnikih, dlančnikih, USB diskih, CDjih, mobilnih telefonih, iPodih in podobnih mobilnih medijih hote ali nehote prenašamo naokrog. Z vedno večjo vlogo brezžičnih omrežij, uporabe brezstičnih tehnologij in prenašanja podatkov v oblake so naše aplikacije in z njimi njihove ranljivosti postale dostopne po zraku. In ker se danes že skoraj vsak računalnik lahko poveže z vsakim, je možnosti zlorabe varnostnih napak vedno več. Tako je aplikacijska informacijska varnost postala zapletena samostojna panoga, ki jo velikokrat izvajajo neodvisno od IT. Lastniki programske opreme, ki jih zakonodaja in uporabniki zavezujejo k izgradnji zelo varnih sistemov poslovne inteligence, praviloma niso v stanju, da bi naročili dovolj varno programsko opremo in na koncu tudi potrdili, da so dobili to, kar so naročili. Ker so po sili razmer velikokrat podvrženi vplivu trgovcev, se pogosto dogaja, da drago kupujejo programsko opremo, ki pa ob prvi priliki podleže zelo preprostim napadom. Pri nas tudi opažamo, da je v življenjskih ciklih aplikacij sorazmerno malo kritičnega, neodvisnega varnostnega preverjanja, zato je programska oprema še bolj ranljiva in izpostavlja osebne podatke in poslovne skrivnosti uporabnikov.

Kljub precejšnjemu napredku pri dvigovanju varnostne zavesti javnosti in skrbi za zasebnost, ki smo mu v zadnjih letih priča, pa tudi razvoju in obstoju mednarodno priznanih varnostnih standardov ter dobrih praks in zakonodajni podpori, obstaja velik razkorak med tem, katere procese bi naročniki in izvajalci morali izvajati in kaj v resnici počnejo. Tudi pogodbenih dogovorov, ki bi jasno določali odgovornost za odpravljanje ranljivosti ter poplačilo škod, nastalih kot posledica vdorov v računalniške sisteme, je pri nas, pa tudi v tujini, zaenkrat še malo, vdorov pa vedno več. Vgradnja varnostnih mehanizmov ter vzdrževanje varne infrastrukture znatno povečata stroške razvojnih projektov, zato se naročniki praviloma odločajo za varnostne investicije kot rezultat (velikokrat napačnih) ocen tveganj, po očitnih krajah podatkov in večjih vdorih v računalniške sisteme, pa tudi po načelu minimalne dolžne skrbnosti (»due diligence«). Gre za prve pomembne korake, a rezultati le-teh ob načrtnem napadu na informacijski sistem praviloma ne morejo zadržati ciljanih napadov visoko usposobljenih in finančno motiviranih posameznikov. Če je včasih veljalo, da je aplikacija varna, če ima vgrajeno dovolj veliko število varnostnih mehanizmov, je danes potrebno, da mora zdržati napade zlonamernih napadalcev – da je torej čim manj »varnostno luknjasta«.

Izvajalci in naročniki se pri gradnji varnih sistemov za poslovno inteligenco oklepajo izgovorov, zaradi katerih se velikokrat zavestno odločajo za manj varne izvedbe svojih aplikacij. Izvajalci se izgovarjajo, da popolne varnosti ni, zato so tudi manj resni pri

odkrivanju in odpravljanju ranljivosti, tudi tistih izjemno nevarnih in onih, ki jih je sorazmerno lahko odkriti. Prav tako velja splošno mnenje, da graditelji vedo največ o svojem sistemu, pri čemer pozabljajo, da je dovolj, da dobro trenirani napadalci najdejo eno samo napako, pa je varnost podatkov kompromitirana za vedno. Tako jim je težko odkriti tudi osnovne varnostne napake, čeprav jih v teoriji dobro poznajo, kaj šele, da bi redno sledili razvoju novih vrst napadov in spremljanju na novo odkritih vrst ranljivosti. Še največ škode pa naredimo s tem, da krepimo močne varnostne člene in ne najšibkejših. Z vgradnjo najsodobnejše varnostne tehnologije samo neoptimalno zapravljamo sredstva, saj bodo napadalci še vedno prihajali v sistem po šibkih členih. Zato je potreba po modelu strategije gradnje varnih sistemov poslovne inteligence, ki je bil ključni cilj raziskovalnega projekta, predstavljenega v prispevku, vedno večja.

1.1. Namen in cilji raziskovalnega projekta

V raziskovalnem projektu smo razvijali preprost model – strategijo za gradnjo varnih sistemov poslovne inteligence, ki ne bi temeljila na slepi vgradnji varnostnih mehanizmov ter definiranju dostopov uporabnikov, temveč na varnostnih aktivnostih, sistematično vgrajenih v življenjski cikel gradnje programske opreme. Model upošteva dejstvo, da imajo različne aplikacije iz različnih razlogov različne varnostne potrebe, kar pomembno vpliva na izvajanje projektnih aktivnosti. Na podlagi dejanskih varnostnih potreb sistema poslovne inteligence je v model vgrajeno znanje o potrebnih aktivnostih za zagotovitev potrebnega varnostnega nivoja v obliki preprostega seznama aktivnosti, ki v določenih delih razvojnega cikla prinašajo največje učinke.

Na podlagi izvedenega modela za strategijo varnih sistemov poslovne inteligence smo izvedli testno analizo na reprezentančnem vzorcu projektov, za katere smo lahko pridobili vse potrebne informacije. Izkazalo se je, da nam je največ verodostojnih in primerljivih podatkov dostopnih pri javnih naročilih IT projektov, ki smo jih uporabili za izvedbo analize. Rezultati so v zgoščeni obliki predstavljeni v prispevku.

Eden od ciljev raziskovalnega projekta je bil prva primerjava razvojnih IT projektov na podlagi modelnih metrik. Nenazadnje pa z raziskavo in prispevkom želimo spodbuditi naročnike varnostno kritičnih sistemov poslovne inteligence, da v proces naročanja od samega začetka vključijo optimalne aktivnosti izvajalcev za večjo varnosti programske opreme.

1.2. Opis uporabljenih modelov in dobrih praks

Gradnja varne programske opreme je izjemno velik izziv za v računalništvu izkušene razvojne ekipe, zato lastniki in izvajalci varnostno kritičinih sistemov poslovne inteligence pospešeno povprašujejo po njim na kožo pisanih metodologijah in standardih, po katerih bi lahko ugotavljali potrebo po primernem varnostnem nivoju programske opreme, vodili in nadzorovali proces izvedbe ter na koncu preverili primernost končne izvedbe sistema. Čeprav so metode, ki bi lahko pomagale pri tem procesu, po delčkih na razpolago v različnih varnostnih standardih, smernicah, metodah in dobrih praksah, pa je iz teh koščkov skoraj nemogoče sestaviti učinkovit kuharski recept, ki bi pomagal pri odločitvah. Metode, ki so danes na razpolago, so precej težko uporabljive, saj so ali preveč tehnične, presplošne, preveč široke, v fazi razvoja ali preveč podrobne in kot take neobvladljive. Kljub vsemu pa je možno nekatera znanja iz obstoječih metodolgij dodobra izkoristiti tudi v službi naročnikov. Tako smo se pri izvedbi modela strategije gradnje varnih sistemov poslovne inteligence oprli tudi na nekatere že obstoječe rešitve.

Splošni varnostni standardi, kot so skupina ISO2700x, PCI DSS[1], COBIT, pa tudi NIST's 800-53[3] in SANS CAG (Consensus Audit Guidelines) [2], lahko tako predstavljajo prvi pomembni korak pri zavarovanju programske opreme. Dobra stran takih splošnih varnostnih standardov je, da jih je že spoznalo in jih vsaj delno uporablja že veliko podjetij, ki so tudi z njihovo pomočjo dvignila splošni varnostni nivo organizacij in zaposlenih v njih. Problem širokih pristopov, ki jih ponujajo splošni varnostni standardi, je v tem, da jih podjetja solidno izvedejo do točke, ko vsaj delno popišejo osnovna varnostna načela, sredstva in grožnje, ustavi pa se pri dejanski izvedbi varnostnih mehanizmov in preverjanju delovanja le-teh, zato bi taka podjetja le stežka uspešno preživela resno revizijo, kaj šele napad. Ti standardi tudi zagotavljajo celovit varnostni pristop organizacij, zato se ne spuščajo v veliko potrebnih podrobnosti, tako da za naš namen – nadzor nad gradnjo varnih aplikacij – ne morejo pokriti celotnega spektra nujno potrebnih aktivnosti.

Drugo skupino standardov predstavljajo **zrelostni aplikacijsko-varnostni modeli**. Ker se je pokazalo, da splošni varnostni standardi pri gradnji varne programske opreme niso dovolj konkretni, so med varnostnimi strokovnjaki začele nastajati pobude o varnostno zrelih organizacijah, ki bi svojo Postopno bi spreminjali celotno organizacijo in zaposlene tako, da bi korakoma dvigovali zavest o varnosti programske opreme po nivojih. Izkazuje se, da gre za visoke, a težko dosegljive cilje, saj je spreminjanje celotne organizacije izjemno naporno delo, ki zahteva vpletenost vseh zaposlenih, spreminjanje obstoječih procesov in avtomatizacija le-teh, kjer je le možno. Zrelostni proces je praviloma drag in počasen, zato takojšnjih velikih učinkov na aplikacijah, ki jih razvijamo, ni za pričakovati. Tako marsikatera organizacija izgubi začetni zalet in kljub veliko truda ostane na nizkih zrelostnih nivojih. Pojavlja se tudi vprašanje, kako učinkovite so tako široko zastavljene aktivnosti, če jih nismo uspešno potrdili na posamezni aplikaciji. Prav tako je vsaj vredna razprave ena od predpostavk, da se visoki nivoji zrelosti organizacije izkazujejo v čim večji avtomatizaciji, sploh, ker zaenkrat modeli ne posvečajo pozornosti sistematičnemu spremljanju in vključevanju novih vrst ranljivosti in napadov, kar pomeni, da bi tovrstna avtomatizacija uspela odkrivati le najbolj specifične in ne posebej zahtevne varnostne probleme. Kljub vsemu predstavljajo zrelostni aplikacijsko-varnostni standardi in dobre prakse odlično podlago za utrjevanje aplikacijske varnosti na vseh področjih gradnje le-teh, saj se prvič sistematično ukvarjajo z vsemi fazami varnega razvoja in tako prerastejo pomanjkljivosti splošnih varnostnih standardov – pomanjkanja konkretizacije in naključni pristop. Pri gradnji modela smo tako upoštevali OWASP SAMM[4] (Software Assurance Maturity Model) in BSIMM[5] (Building Security in Maturity Model).

Največ pričakovanja po hitrih in učinkovitih pristopih za gradnjo varnih aplikacij nam predstavljajo **specializirani aplikacijsko-varnostni pristopi**. Od njih si želimo konkretnost, usmerjenost k tehničnim napotkom brez odvečnih organizacijskih ter promocijskih vložkov in takojšnjo uporabnost na nivoju posameznih projektov. Namenjeni so vsakodnevni uporabi celotne razvojne ekipe. Zaradi tako visokih pričakovanj zaenkrat še ne moremo pričakovati, da bomo kmalu prišli do učinkovitih standardov, tudi zaradi tega, ker so na tehničnem nivoju aplikacije in uporabljene tehnologije izjemno raznolike in jih bomo težko pospravili pod en dežnik. A vendar vsak zase prispevajo košček sestavljanke k višji varnosti sistemov poslovne inteligence. Na tem mestu omenimo standard ISO 15408[6] (Common Criteria, CC), uporabljan za definiranje poslovno-varnostnih zahtev, OWASP ASVS (Application Security Verification Standard) za varnostno preizkušanje spletnih aplikacij ter Microsoft SDL (Security Development Lifecycle), ki velja za najbolj zrelega in uporabnega med vsemi. Stroka že dalj časa nestrpno pričakuje standard ISO 27034 (Guidelines for application

security), ki je še daleč od izdaje. V to skupino uvrščamo tudi model za gradnjo varnih sistemov poslovne inteligence.

2. OPIS ZASNOVE MODELA STRATEGIJE GRADNJE VARNIH SISTEMOV POSLOVNE INTELIGENCE

Model strategije gradnje varnih sistemov je namenjen hitremu in učinkovitemu nadzoru varne gradnje velikega števila aplikacij, zato mora biti proces ocenjevanja preprost. Uporabnik modela si v splošnem zastavi tri ključna vprašanja:

1. Kakšen nivo varnosti zares potrebujemo?
2. Smo načrtovali ključne aktivnosti za doseganje določenega varnostnega nivoje?
3. Smo pred uporabo izvedli vse zahtevane ključne varnostne aktivnosti željenega varnostnega nivoja?

Odgovore na vprašanja poiščemo s pomočjo dveh vprašalnikov. V vprašalniku »Ciljni aplikacijski nivo varnosti (CANV)« določimo potrebo po nivoju informacijske varnosti v aplikaciji, kar naredimo v 1. koraku. Ocena CANV je izražena kot vrednost med 0 in 6, pri čemer 0 predstavlja manjše varnostne potrebe in 6 najvišje.

V nadaljnjih korakih izpolnjujemo vprašalnik »Ocenjeni aplikacijski nivo varnosti (OANV)«, ki govori o načrtovanih in izvedenih varnostnih aktivnostih pri gradnji sistema poslovne inteligence, glede na fazo razvojnega življenjskega cikla. Oceno OANV primerjamo z oceno CANV ter tako ugotovimo odstopanja načrtovanih ali dejanskih varnostnih aktivnosti od željenega varnostnega nivoja.

Prvotna različica modela je že bila predstavljena strokovni javnosti [8], vendar je model od takrat doživel nekaj večjih nadgradenj. Oba vprašalnika (CANV in OANV) sta v celoti javnosti na razpolago na spletni strani www.acros.si.

V nadaljevanju si od bližje poglejmo odgovore na vsa tri ključna vprašanja.

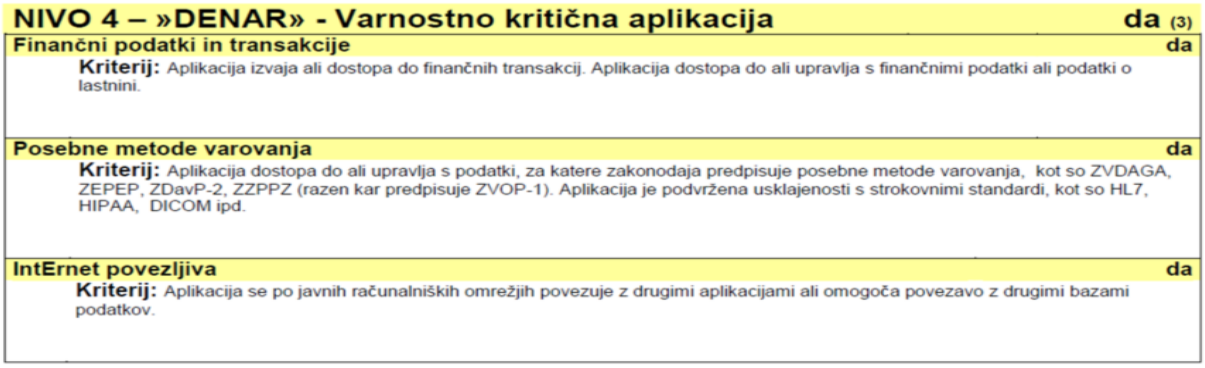
2.1. 1. korak: določitev ciljnega aplikacijskega nivoja varnosti (CANV)

1. korak (izpolnitev vprašalnika CANV) izvajamo v času določitve varnostnih zahtev, še preden razmišljamo o varnostni arhitekturi ali posameznih izvedbenih podrobnostih. Kljub veliki razpoložljivosti različnih varnostnih mehanizmov ne bi imelo pravega smisla, da bi bila prav vsaka programska oprema zgrajena na popolnoma varen način in da je vsa programska oprema enako varna. Za marsikatero aplikacijo niti ne pričakujemo, da je grajena popolno, je pa nujno, da ocenimo, kak nivo varnosti dejansko potrebuje. Taka ocena je izjemno pomembna pri določanju aktivnosti, ki so potrebne za doseganje določenega dejanjskega varnostnega nivoja. Ključni kriteriji za ocenjevanje varnostnih potreb aplikacije ne bodo število in sofisticiranost varnostnih mehanizmov ali uporabniki, temveč predvsem vrsta podatkov, dostop, upravljanje z zasebnostjo in poslovnimi skrivnostmi, vrste uporabljenih tehnologij, število potencialnih uporabnikov, povezljivost, zakonske zahteve, ali aplikacija lahko ogroža premoženje, zdravje ali življenje ljudi in podobno.

V grobem lahko aplikacije popredalčakamo v naslednje nivoje od 0 do 6: “0. Nima varnostnih zahtev”, “1. Osnovna varnost”, “2. Javni dostop”, “3. Podatki”, “4. Denar”, “5. Skrivnost”, “6. Življenje”

Vprašalnik za vsak aplikacijski nivo postavi dva ali tri vprašanja, na katera so možni odgovori: da, ne, ni podatka. V primeru, da je katerikoli odgovor na vprašanje nivoja pritrdilen, velja, da je ocena CANV za aplikacijo najmanj toliko, kot je številka nivoja. CANV ocena aplikacije je najvišja številka nivoja, kjer je bil katerikoli odgovor pritrdilen.

Slika 1: Primer iz vprašalnika CANV prikazuje vprašanja, ki jih za 4. nivo zastavljamo v vprašalniku CANV. V primeru, da je katerikoli odgovor na vprašanje nivoja pritrdilen, je CANV ocena aplikacije najmanj številka nivoja (v našem primeru 4).



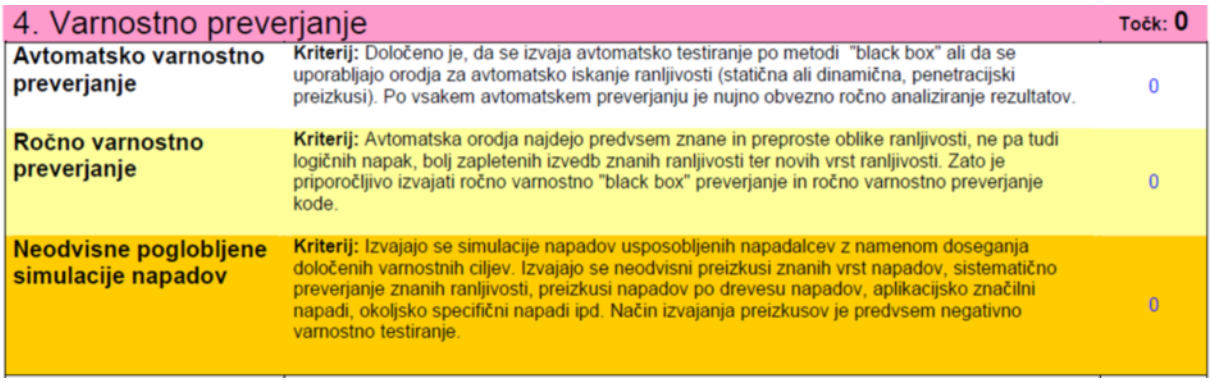
Slika 1: Primer iz vprašalnika CANV

2.2. 2. korak: določitev ocenjenega aplikacijskega nivoja varnosti (OANV) v času naročanja izvedbe in pred prevzemom sistema v uporabo

Ocenjen aplikacijski nivo varnosti ugotavljamo skozi določevanje skupin aktivnosti, ki jih delimo med **ključne aktivnosti** (»1. pogodbene zaveze«, »2. Varnostne zahteve«, »3. Varnostna arhitektura«, »4. Varnostno preverjanje«) in **druge aktivnosti** (»5. Ljudje«, »6. Varno kodiranje«, »7. Preverjanje varnostnih funkcij«, »8. Ključne ranljivosti«, »9. Metrike«, »10. Varnostni standardi in prakse«).

Za vsako skupino aktivnosti odgovarjamo na 3 vprašanja o načrtovanih ali izvedenih aktivnostih in za odgovore prejmemo točke, ki so glede na dejanski vpliv aktivnosti na varnost obtežena (1 točka za manjši vpliv, 2 točki za srednji vpliv, 3 točke za največji vpliv). Za skupino aktivnosti lahko tako zberemo največ 6 točk za aplikacijo.

Ker se zavedamo finančnih, tehničnih in časovnih omejitev naročnikov, predlagamo, da se v prvi vrsti izvedejo ključna področja, za bolj varnostno kritične aplikacije pa tudi druge potrebne aktivnosti. Ključna področja so izbrana tako, da pokrijejo celotni življenjski cikel razvoja programske opreme. Prav tako smo skozi obravnavo ključnih področij spodbujeni, da se vprašamo, kaj v resnici potrebujemo in ali smo to na koncu tudi dobili. Druga področja pomagajo pri izvedbi sekundarnih varnostnih aktivnosti in povečujejo nivo zaupanja v dejansko varnost programske opreme.



Slika 2: Primer iz vprašalnika OANV

Slika 2: Primer iz vprašalnika OANV prikazuje vprašanja, ki jih za 4. aktivnost (Varnostno preverjanje) zastavljamo v vprašalniku OANV. Za pritrdilni odgovor za "Avtomatsko varnostno preverjanje" bi prejeli 1 točko, za "Ročno varnostno preverjanje" 2 točki in za "Neodvisne poglobljene simulacije napadov" 3 točke, skupaj največ 6.

2.3. 3. korak: preverjanje, ali smo z aktivnostmi dosegli željeni nivo

Idealno bi bilo, če bi pri prav vsaki skupini aktivnosti (tako ključne kot druge) zbrali vsaj tako OANV oceno, da bi bila vsaj enaka, če ne večja aplikacijskemu CANV nivoju. Po zasnovi modela pričakujemo, da aplikacija za vsako skupino ključnih aktivnosti zbere vsaj toliko točk, kot je njena CANV ocena, da so aktivnosti primerno obtežene z željenim ciljnim nivojem aplikacijske varnosti.

3. IZSLEDKI RAZISKAVE UPORABE MODELA STRATEGIJE GRADNJE VARNIH SISTEMOV POSLOVNE INTELIGENCE

3.1. Opis uporabljenega projektnega testnega vzorca

Nivo ciljne aplikativne varnosti je potrebno določiti v času določanja poslovnih zahtev. Prav tako je potrebno v času naročanja izvedbe podrobno razumeti, načrtovati in naročiti ključne aktivnosti, ki so potrebne, da aplikacije in celotni sistem zgradimo na dovolj varen način. Zato smo v testne namene uporabili javne dostopne podatke javnih naročil IT projektov, saj smatramo, da so v času naročanja zelo primerni za uporabo metodologije. Ob določitvi končne cene izvedbe bi v idealnem primeru že zahteve morale vsebovati dovolj jasno definirane varnostne predpostavke, aktivnosti in varnostne cilje, saj je to edini način, da jih bodo izvajalci lahko vključili v ponudbe.

Referenčni seznam za izgradnjo seznama testnih projektov javnih naročil so predstavljale javne objave v obdobju 1.1.2009 – 30.9.2009 na spletnem portalu www.enarocanje.si [7] in referenčne povezave na nadaljnjo dokumentacijo. V prvotno raziskavo smo vključili javne IT projekte, ki so v obdobju analize javno objavili naročilo, popravek naročila, objavo izbora ali preklic naročila. Smatramo, da smo na ta način v raziskavi zaobjeli širok referenčni vzorec kompleksne programske opreme, ki mora biti zgrajena primerno varno. Zaradi izjemne pomembnosti bodočega IT projekta za slovensko družbo smo na seznam vključili tudi dokumentacijo povabila k strokovnemu dialogu za projekt zVEM (december 2009).

Projekte s seznama smo ovrednotili tako po vprašalniku »Ciljni aplikacijski nivo varnosti (CANV)« kot tudi po vprašalniku »Ocenjeni aplikacijski nivo varnosti (OANV)«, pri čemer smo le-tega ocenjevali do definiranja zahtev. Informacij o oceni CANV po zaključku projekta ne moremo podati objektivno, saj ima popolno dokumentacijo o tem le naročnik, prav tako večino analiziranih projektov v času izvedbe raziskave še ni bilo zaključenih. Prav tako se zavedamo omejitev raziskave na javno objavljeno dokumentacijo, a le tako smo lahko zagotovili pošteno primerjavo med projekti. Na podlagi referenčnega vzorca smo izračunali povprečno CANV in OANV oceno ter analizirali nekatere ključne odgovore.

Tako smo pridobili prve referenčne rezultate analize dejanskih (praviloma varnostno kritičnih) projektov, ki so testno ocenjeni na enak način in med seboj primerljivi. Sklepamo, da gre za prvo tovrstno analizo v Sloveniji, prav tako v času izvedbe analize nismo naleteli na podobne raziskave v tujini. Ker se je izdelan raziskovalni mehanizem izkazal za zelo uporabnega, izvajamo analizo tudi na projektih, ki jih v javni upravi naročajo tudi po

30.9.2009. Tako gradimo bazo referenčnih projektov tudi še po uradnem zaključku raziskave. Rezultati, prikazani v članku, predstavljajo prerez na datum 31.12.2009.

Projekte, ki jih analiziramo, smo določili v treh korakih. V prvem koraku smo pripravili seznam vseh naročil na področju IT (132), ki smo ga omejili na seznam ocenjevanih (37). Med ocenjevanimi smo izpostavili 13+1 projektov (Tabela 1), za katere smatramo, da so izjemno varnostno pomembni. Za te smo dodatno komentirali naše ocene ter obvestili naročnike in jim ponudili dodatno razlago analize.

Število projektov	**Opis projektov**	**Aktivnost**
132	• Vsa javna naročila strojne in programske opreme • Tudi javna naročila s pogajanji (ni dokumentacije) • Tudi nakup licenc	Evidentiramo
37	• Projekti z javno dostopno dokumentacijo • Naročila večjih vrednosti (>500.000 EUR) • Nekaj izjem (deli sklopov, pomembni podatki, povezljivost)	Ocenjujemo »*Skupina (37)*«
13+1	• Največja naročila gradnje aplikacij *eDIS, eZK, ISPEK, Informatizacija vpisnikov, IS za šolske zavode, Nadgradnja e-VEM, Poslovni IS za JHL, Prenova CKE, Prenova IS (KCLJ), SICIS, Sistemska podpora MJU, Skupna kmetijska politika do 2013, Vpogledovalnik v zbirko vrednotenja nepremičnin* • Upravljanje z varnostno kritičnimi podatki • +1: povabilo k strokovnemu dialogu (zVEM)	Ocenjujemo, komentiramo, obvestimo naročnika *»Skupina (13+1)«*

Tabela 1: Določitev projektov za analizo

3.2. Povzetek analize CANV in OANV

Analiza ocen CANV je pokazala, da v povprečju javna naročila presegajo ciljni nivo 4, pri čemer je CANV povprečje »Skupine (13+1)« pričakovano višje od »Skupine (37)«. Ugotavljamo, da je ocena CANV visoka zaradi skoraj neizogibnega upravljanja osebnih podatkov državljanov v javni upravi. Bodoče aplikacije v javni upravi so tudi zelo povezljive (na Internetu in Intranetu), kompleksne in so instalirane na računalnikih, ki so povezani v Internet.

a) število projektov na CANV nivoju

Nivo	**37**	**13+1**
Povprečni CANV	**4.35***	**4.93**
1. "Osnovna varnost"	33	14
2. "Javni dostop"	21	12
3. "Podatki"	32	13
4. "Denar"	33	14

b) najpogostejši odgovori CANV

Št. odg.	**Kazalnik**
23	Dostop do os. podatkov
21	Intranet povezljiva
21	Internet povezljiva
20	Kompleksna
20	Aplikacija na računalniku z dostopom do Interneta

5. “Skrivnost”	17	8
6. “Življenje”	8	5

19	Finančni podatki in transakcije
14	Veliko uporabnikov

Tabela 2: Rezultati CANV – a) število projektov na CANV nivoju, b) najpogostejši odgovori CANV

Analiza ocen OANV je pokazala na aktivnosti, ki jih naročniki pri javnih naročilih naročajo najpogosteje in ki jih sploh ne naročajo. Med ključnimi aktivnostmi jih največ pozornosti posveča določanju varnostnim zahtevam (zaradi zahtev po izvedbi varnostnih in revizijskih funkcionalnosti), med drugimi aktivnostmi pa uporaba varnostnih standardov in praks.

a) po skupinah aktivnosti

OANV aktivnosti	***37***	***13+1***
KLJUČNE AKTIVNOSTI		
1. Pogodbene zaveze	0,5[1]	1,2
2. Varnostne zahteve	1,9	2,2
3. Varnostna arhitektura	0,1	0,2
4. Varnostno preverjanje	0,0	0,1
DRUGE AKTIVNOSTI		
5. Ljudje	0,1	0,0
6. Varno kodiranje	0,0	0,0
7. Preverjanje varnostnih funkcij	0,0	0,1
8. Ključne ranljivosti	0,0	0,0
9. Metrike	0,2	0,4
10. Varnostni standardi in prakse	0,3	0,5

b) po posameznih aktivnostih

OANV aktivnosti	***37***
NAJVEČKRAT NAROČANE AKTIVNOSTI	
Varnostne funkcionalnosti določene	28
Določene revizijske funkcije	22
Uporaba splošnih varnostnih standardov	8
Preverjanje usklajenosti varnostnih zahtev z zakonodajo	7
Odgovornost za ranljivosti	6
DRUGE AKTIVNOSTI	
Varnostni profil	3
Zahteva po sodelovanju varnostnega strokovnjaka	2
Projektni člani varnostno usposobljeni, varnostno usposobljene skupine, načrtovano testiranje varnostnih funkcionalnosti, avtomatsko varnostno preverjanje	1

Tabela 3: Najpogostejši odgovori OANV a) po skupinah aktivnosti; b) po posameznih aktivnostih

Nadaljnja analiza rezultatov je pokazala, da naročniki v svoje zahteve ne zapisujejo nekaterih ključnih aktivnosti, ki bi bistveno povečala končno varnostno stanje sistema poslovne inteligence. Tako v celotnem testnem vzorcu nismo zaznali načrtovanja aktivnosti, kot so določitev varnostnih mejnikov in metrik, določeno ciljno varnostno stanje, arhitekturni model groženj, določitev in redukcija področja napada ("attack surface") in ročno varnostno preverjanje.

Drugih aktivnosti, ki jih naročniki ne zapisujejo v zahtevnike, je veliko, naj izpostavimo pomanjkanje dobrih varnostno-razvijalskih praks, načel varnega kodiranja, iskanje TOP ranljivosti in zahtev po sodelovanju izkušenih etičnih hekerjev.

[1] Povprečno število zbranih točk za področje (od 6 možnih)

Pričakujemo, da neodvisne poglobljene simulacije napadov naročniki izvedejo neodvisno od javnega naročila, saj jih zaradi zahtevane neodvisnosti ne more izvesti izbrani izvajalec.

4. SKLEP

Model strategije gradnje varnih sistemov poslovne inteligence predstavlja edinstveno naročnikovo orodje za preprosto varnostno kategoriziranje večjega števila svojih aplikacij v sistemih poslovne inteligence in omogoča določevanje potrebnih optimalnih varnostnih aktivnosti. Skozi analizo uporabljenega projektnega testnega vzorca se je pokazal za zelo primerno orodje za obvladovanje varnostnih zahtev v zelo kompleksnih sistemih.

Ugotavljamo, da bo sam model v prihodnjem deležen nekaterih nadgradenj: dodane bodo nekatere nove varnostne aktivnosti, prav tako smo po raziskavi ugotovili, da bi bilo primerno ponovno oceniti primernost uteži (števila točk) za nekatere od aktivnosti.

Za raziskovalno ekipo je bil eden večjih izzivov dovolj poglobljeno spoznati vse testne projekte, kar je tudi predstavljalo večji del dela pri analizi le-teh. Po pogovorih z nekaterimi naročniki smo tudi ugotovili, da se včasih v procesu izbiranja najprej izbere cena in izvajalec in šele naročniki določijo ali izločijo nekatere varnostne aktivnosti tudi po izbiri izvajalca

Ker nobeden od analiziranih projektov pri oceni OANV za vse ključne aktivnosti ni prejel več kot 0 točk, primerjave med CANV in OANV na projekt nismo izvajali. Izziv za bodoče raziskovanje predstavlja tako ugotavljanje odnosov med oceno CANV in posameznimi aktivnostmi, prav tako povezava med posameznimi zakonodajnimi obveznostmi in aktivnostmi.

Kljub vsem možnostim izboljšav ocenjujemo, da gre za edinstven model strategije za gradnjo varnih sistemov poslovne inteligence, prav tako smo z rezultati analize dobili prvi sistematični pogled na naročanje varnostnih zahtev v projektih javne uprave. Upamo, da bodo projektni rezultati naročnikom olajšali delo in vzpodbudili k še bolj doslednemu določanju pravih varnostnih zahtev in potrebnih ključnih varnostnih aktivnosti.

5. ZAHVALA

Ministrstvu za visoko šolstvo, znanost in tehnologijo RS ter podjetju ACROS d.o.o. se zahvaljujem za financiranje raziskovalnega projekta.

6. VIRI IN LITERATURA

[1] PCI-DSS, https://www.pcisecuritystandards.org/

[2] SANS Consensus Audit Guidelines, http://www.sans.org/cag

[3] NIST's 800-53, http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

[4] OWASP SAMM in OWASP ASVS, http://www.owasp.org

[5] BSIMM, http://www.bsi-mm.com/

[6] ISO 15408 (Common Criteria), http://www.commoncriteriaportal.org/

[7] Portal javnih naročil: www.enarocanje.si, Uradni list RS

[8] ŠALAMUN, Stanka: 3 kilograme aplikacijske varnosti, prosim!, 17. mednarodna konferenca o revidiranju in kontroli informacisjkih sistemov, zbornik str. 99 – 116